Access Control Equipment and Electronic Security

Summary

As security concerns continue to soar throughout the world since the attacks of September 11, 2001, the fast-changing Canadian access control systems market presents extremely strong potential for U.S. exporters. Advanced American security technology has allowed U.S. firms to offer products that are more efficient and effective relative to their counterparts in Canada.

The total market in Canada for access control equipment for 2005 was approximately US $532 million, with a growth potential of 8-10 percent predicted through 2008. Since Canadian companies focus on export, the market is over 95 percent dominated by imports, and U.S. imports of US $217 represented 41 percent of the total Canadian market in 2005. While the market includes locks, keys, automatic garage doors and alarm systems, the growth in the market will continue to be in electronic physical access control systems, led by biometric, smart card and other non-contact technology together with software that can used to secure both physical access to facilities and access to data stored on computers.

The main end users of access control and electronic security equipment are industrial facilities, defense installations, airports, and other governmental facilities, followed by banks and other financial institutions. Selling to the Canadian Government involves the public procurement process, while he commercial sector purchases access control security systems by commercial negotiations with well-established distributors, agents, and manufacturer's representatives. Access control products may need to comply with Canadian standards including the new standard CAN/ULC-S319-05, Electronic Access Control Systems, as well as French language requirements for sale in Quebec. If the Quebec rules are followed, companies will meet all the bilingual rules that may be applicable for sales in the other provinces. Exporters are encouraged to work with a local distributor or major retailer to meet these requirements and ensure proper French-Canadian language usage.

Sales of access control products to Canadian companies are handled through relatively short marketing channels, and in some cases products move directly from manufacturer to end-user. Canadian companies have a strong preference for vendors with a local presence either directly or through a partner. U.S. suppliers of access control equipment should consider locating a reliable distributor who will sell to an electronic product retailer that deals exclusively in safety and security.

No customs duties or tariffs are levied on qualified U.S.-made access control systems entering Canada. The Canadian Goods and Services tax (GST) of 7 percent on a value-added basis is assessed by Revenue Canada at the time of import, but may be refundable upon resale.

Market Demand

The access control equipment and electronic security market is a sub-sector of the larger safety and security equipment market, comprising both mechanical and electric/electronic security equipment. For purposes of this report, generic electronic equipment used for access control such as television cameras, still image video cameras and video camera recorders, and components for such equipment, are excluded.

Access control to physical facilities includes a wide variety of technologies well-accepted in Canada for residential, commercial, institutional and government use, including the following:

- traditional locks and keys and their newer electronic replacements, such as found at most large hotels
- intercoms and video systems for remote door-opening
- alarm systems and other technologies for intrusion detection
- bullet and blast-resistant glass security products.

Products such as the above in this mature sector of the market will most likely keep a presence in the market due to legacy systems and high user familiarity.

Increasingly, in Canada, as elsewhere, access control systems are incorporating smart cards and biometric identification or non-contact technologies such as Radio Frequency Identification (RFID). The expansion of this market has brought price reductions that have allowed the sale of smaller systems controlling from two to 16 doors using technology formerly only feasible for larger systems.

Canadian firms are also starting to follow the current trend of adopting one technology to secure both physical access to facilities and access to data stored on computers, such as by use of smart cards and biometrics identification, utilizing the same card for both purposes. Demand for this technology will be a prime moving force behind the expected growth rate of the market for access control equipment in Canada of approximately 8-10 percent per year through 2008. However, the complexity and costs of adopting such systems still inhibit their more widespread diffusion in Canada.

But the Canadian market is changing fast. The website of SP&T News, a leading information source on Canada's security industry, has indicated that keeping current on Canada's security industry is a daunting task:
Today, reporting on the Canadian security industry is harder than ever. Besides keeping tabs on the Fortune 100 companies — GE, Honeywell, Tyco, Ingersoll-Rand, Bosch, United Technologies Corp., just to name a few — that have chosen the security industry as an arena to toil in, it has been amazing, and sometimes confusing, to keep track of security technology that is evolving at break-neck speeds, new products that are being released into the marketplace on a daily basis, and new security-focused companies that are infiltrating the market place from all four corners of the world, not to mention new industry sectors (e.g., IT).

Although the Canadian access control market is considerably smaller than that of the United States, Canadian security concerns tend to echo U.S. patterns. This helps explain the success of U.S. access control firms in Canada, and underscores a competitive advantage that can be exploited by U.S. firms interested in expanding their business to Canada. For example, when security concerns in Canada began to rise steadily after the September 11 tragedy, the U.S. access control industry was one step ahead of Canada in developing the necessary technologies for Canadian consumers to deter threats. In addition, the close geographic proximity of the United States to Canada allows U.S. firms to provide technologically advanced equipment at competitive prices, and supply attractive customer service and technical support to Canadian dealers and end users. Overall, U.S. suppliers of access control equipment face the challenge of responding to two major requirements of Canadian consumers: (1) technologically advanced products that can ensure control over people and products and access to facilities; and (2) price-competitive products in an industry that is becoming increasingly competitive.

Following the increased security concerns since the September 11, 2001 terrorist attacks, the Canadian government has recommended that corporations, airports, hospitals, and other public and private facilities implement advanced security technologies to improve safety. The Canadian government has also allocated significant resources to the procurement of these technologies for public purposes. In particular, biometrics and smart cards have been identified as key access control technologies. The Canadian government has been a pioneer in the adoption of smart card technology. Canada's Passport Office is currently considering implementing facial recognition biometrics by 2007.

Security has thus become a top-level concern as firms are beginning to realize the importance of protecting their employees and their assets from internal and external threats. Similarly, major Canadian insurance companies are now establishing increasingly stringent security standards that businesses must follow to qualify for insurance. The unstable climate ushered in by terrorism and the skill of identity thieves, industrial spies and other intruders to out-smart access control technologies have forced Canadian businesses to continually update or purchase new access control systems that provide leading-edge security control. Canadian businesses use security cards employing a wide variety of technologies: bar code, embossed, infrared, laser/holograph, magnetic stripe, optical, proximity (radio, infrared), and "smart" technologies incorporating microchips. These systems typically contain ID card issuance equipment, access control readers at doors or other access points, and door controllers that open the door to authorized users. The most notable change the access control industry has undergone in recent years is the shift to software – enabling access control products to be used as front-ends for entire security systems. Canadian organizations will increase controls on employee credentials wherever possible through smart card technologies. In addition, past studies have revealed that Canadians are very dependent on passwords to access their information -- over 89 percent of Canadians use passwords to accomplish daily tasks such as banking, checking email, turning on PCs and retrieving telephone messages.

Despite privacy concerns over private-sector uses of biometric data, biometrics has excellent market prospects in Canada over the short term, especially in government-issued identity cards. The technology is already in used at the U.S.-Canada land border as part of the bilateral Free and Secure Trade (FAST) program for expediting entry of truck drivers in both directions. Canada's CANPASS Air program to expedite entry into Canada at seven major airports utilizes iris recognition to speed frequent travelers through Customs and Immigration. The Canadian federal government is also considering what biometrics to adopt in developing more secure Canadian passports and citizenship cards over the next several years. Biometrics is also being used for high security applications in the banking, immigration visa processing and law enforcement sectors, increasingly together with personal identification numbers (PINs). Some companies are buying computer keyboards with built-in fingerprint scanners to restrict log-ins to the computer to authorized users. The high rate of construction and industrial development currently taking place across Canada also offers another excellent growth prospect.

The other technology showing rapid growth in Canada is smart cards. Loyalty and gift certificate programs are common smart card uses in the country. Currently smart card technologies are being utilized across Canada for transit, data security, stored value and e-cash, time and attendance, parking payment and other applications.

The demand for smart cards is also expected to be driven by the migration in the Canadian banking sector from magnetic-stripe debit cards to the contactless EMV (Europay-MasterCard-Visa) standard for bankcards to be implemented in stages over the next ten years. This is particularly important in Canada, which has the highest per-capita use of debit cards for point-of-sale purchases in the world, even exceeding credit card use. In 2002, 44 percent of Canadian consumers used debit cards as the primary means of purchase compared to 30 percent who preferred cash. The high use of debit cards also has resulted in increased reports of debit card fraud, which is another driving force behind increased consumer banking security needs calling for better access control technology.

Market Data

While domestic production of access control equipment in Canada has grown slightly in U.S. dollars between 2003 and 2005, this growth has been due almost entirely to the appreciation of the Canadian dollar, as shipments have remained essentially flat. Also, industry estimates reveal that Canadian production, which accounted for 4 percent of Canada's domestic demand in 2005, will meet only 2 percent of domestic market demand in 2006. This is because Canadian producers primarily target foreign markets in order to achieve adequate economies of scale, so that the Canadian market relies on imports to satisfy its growing domestic demand for access control equipment. This has allowed U.S. firms and other foreign producers to control 94-98 percent of the Canadian access control equipment market.

The competitive environment in the access control industry is expected to remain favorable to U.S. firms expecting to expand their business in Canada. U.S. imports into Canada are expected to reach US$ 242 million for 2006. U.S. suppliers will have approximately 40 percent of Canada's total estimated market in 2006 of U.S. $599 million in 2006 and be responsible for 41 percent of Canada's US$ 586 million imports in this sector. Industry forecasts indicate U.S. imports are expected to grow at a real rate of approximately 8-10 percent annually between 2006-2008. The following table provides an overview of the estimated size and growth trends for the Canadian market for access control equipment.

Canadian Market For Access Control Systems
(US$ Millions)

	2004	**2005**	**2006**	**Projected Average Annual Rate 2007-2008**
Canadian Imports	547	512	586	8-12%
Local Production	352	386	487	
Canadian Exports	285	365	475	
Total Market	614	532	599	8-10%
U.S. Imports	274	217	242	8-10%
Exchange Rate	US $1 = CDN $1.30	US $1 = CDN 1.18	US $1 = CDN 1.18	
Inflation Rate	1.90%	2.0%	2.0%	

The rapid integration and technological improvements of products, coupled with the influx of electronic equipment from the Pacific Rim, has tightened competition for electronic access control equipment in North America.

In 2005, the biggest player in the Canadian access control import market after the United States was China, accounting for approximately 18 percent of total imports. Other countries exporting to Canada have much smaller shares of the import market. Mexico holds 10 percent and South Korea controls approximately 8 percent. Imports from China, Mexico and South Korea are concentrated in sales of toughened and laminated safety glass, padlock and alarm systems, and are not a significant source of competition to U.S. companies in the Canadian market for high-value-added access control systems and equipment.

Industry experts state that demand for greater access control will fuel demand for increasingly sophisticated systems. U.S. technology is recognized as a front-runner in technological development in this industry, and therefore, U.S. companies should be in a good position to take advantage of this trend.

Best Prospects

The growth in the market will continue to be in electronic physical access control systems, especially using biometrics, smart cards and contactless technology, which can also be used to secure data system access.

Key Suppliers

The domestic production of access control products in Canada for the industrial, commercial and residential markets occurs primarily in Ontario and Quebec. While Canadian manufacturers are small and control only a small part of the domestic market, they are considered to make high quality products and are generally quite sensitive to customizing products to meet consumers' needs and preferences. However, product selection, technological sophistication and price ranges are limited with Canadian products, creating an avenue for U.S. firms to take to attract Canadian end users.

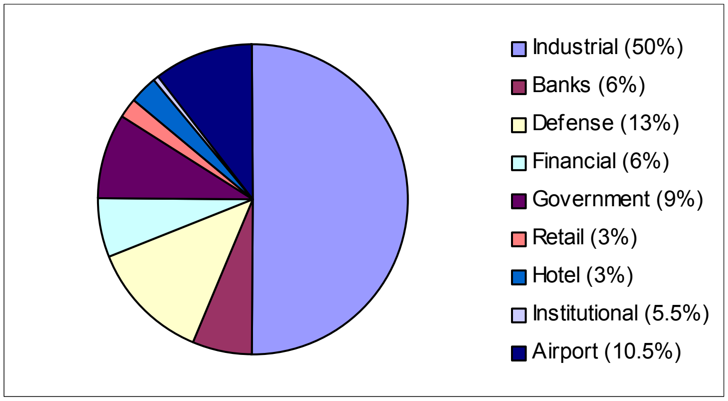
There are three major Canadian manufacturers of access control equipment, Kantech (part of the Tyco Group), Keyscan and Verex (a subsidiary of Chubb Security). Other major players include Digital Security Controls (part of Tyco Fire & Security), and Paradox Security Systems. All these companies ship their products worldwide. In addition, companies such as Acsys Biometrics, Diaphonics and Bioscrypt are examples of the numerous small and new firms that are emerging, primarily in Ontario, with innovative access control technologies, especially in the field of biometrics.

Additional information on Canadian manufacturers and distributors in the access control industry can be found on the Canadian Security Association (CANASA) website at www.canasa.org. This website provides company information on approximately 60 manufacturers and also on 25 distributors, of which a substantial number make or sell access control equipment.

As stated above, there is no significant competition to U.S. companies from companies based in other countries in this subsector.

Prospective Buyers

As shown in the following chart, the main end users of access control and electronic security equipment are industrial facilities, defense installations, airports, and other governmental facilities, followed by banks and other financial institutions.



Industrial facilities, banks, and defense installations have traditionally adopted access control technologies to secure their facilities and data, and are expected to remain the major end users. In addition, increased security concerns following the aftermath of 9/11 have prompted airports, shopping centers, major retailers, casinos, hotels, universities, and hospitals to explore access control security solutions to their facilities and their data to include biometrics and smart card technology. The Canadian government is also moving to make more secure vital personal identification documents, such as by adopting biometrics in passports.

The financial sector has been a major user of smart cards. Canada's seven banks say they want additional smart card standards in place before they migrate their magnetic-stripe credit and debit cards to include chips. Following increasing security threats in terms of identity theft and perimeter violation, many more corporations and organizations are ramping up their security concerns

Additionally, stores and shopping centers are starting to use the newest access control technology. Fingerprint biometrics are useful to retail stores for both secure employee sign-in to a cash register and time and attendance control. These technologies are easy for employees to use and invisible to store customers.

Airports have been among the first movers towards biometrics implementation. While Canadian airports have not invested as heavily in security measures as their counterparts in the United States, they have shown great interest in the industry by purchasing explosives detection devices, digital CCTV cameras, and other access control technologies.

At present, airport employees access restricted areas using their electronic access cards, but the cards do not positively identify the person carrying the card. The Canadian Air Transport Security Agency (CATSA) has therefore been giving biometrics technology a pilot test for restricted area identification cards for employees at four Canadian airports. If successful, use of these cards, which use both fingerprint and iris scans, will be expanded to 150,000 employees at 29 of the country's largest airports.

Hotels are becoming more involved in ensuring security and access control to protect their clientele. Many hotels have moved away from the industry's traditional open-door policy, and have adopted more restrictive measures to prevent security problems. Smart cards, security cameras, and other access controls will continue to be used by hotels in the future.

Canadian college and university campuses are facing many of the same security challenges as other end users. To restrict outsiders from gaining access to student facilities such as dormitories and libraries, many post-secondary institutions have already adopted smart cards, which give their students access to different locations. This trend, reflecting increasing security concerns, is expected to continue in the future. In particular, some campuses are utilizing a system where students and employees both use one integrated smart card, which enables them to access student information, meal plan and library systems, access control, and banking information.

Nonetheless, fewer Canadian universities and colleges have adopted an "all-in-one" smart card on their campuses. Most post-secondary institutions are using smart cards that can only be programmed to allow students or staff to gain access to particular facilities such as meal plans and the gymnasium, but not to banking information. As such, an untapped and potentially lucrative market exists for multi-purpose smart cards.

Similarly, hospitals have begun to take security issues more seriously over the past few years -- particularly in critical areas such as nurseries, pharmacies, and waiting rooms, although hospital managers face fiscal constraints in acquiring additional technology and hiring additional security personnel as they also seek to modernize their medical technology. Although many hospitals already utilize security cameras, and some have installed card systems for restricted area access, some industry insiders state that smart cards could become more popular in this sector in the next few years.

Selling to the Canadian Government involves the public procurement process. The website of Public Works and Government Services Canada gives valuable information on how to sell to the Canadian government. The Canadian government's official Internet-based electronic tendering service MERX gives subscribers access to more than 1,500 open tenders from the federal government, provincial governments, and many municipalities, school boards, universities, and hospitals that are subject to Canada's trade agreements.

The commercial sector purchases access control security systems by commercial negotiations with well-established distributors, agents, and manufacturer's representatives. Personal relationships can greatly influence the success of a U.S. company in this market. This is very important for new-to-market companies.

Market Entry

Sales of access control products to Canadian companies are handled through relatively short marketing channels, and in some cases products move directly from manufacturer to end-user. While some manufacturers choose to sell directly to clients with their own sales force and distribution operations, others use different combinations of distributors, general sales agents, and manufacturers' representatives. When setting up a distribution network in Canada, U.S. manufacturers should consider establishing representation in different regions of the country.

Canadian companies have a strong preference for vendors with a local presence either directly or through a partner. Partnering with a Canadian-based security company that caters to outsourcing, consulting, or systems integration is a quick and cost-effective way to reach a large customer base. According to a Canadian Security survey, most Canadians indicated that they would prefer to buy an access control system from a dealer who is a well-known professional in the security business and who has a strong reputation for providing quality products and services. Thus brand recognition is extremely important to Canadian consumers who are careful about who they deal with and may be skeptical toward newcomers. For this reason, new market entrants should carefully evaluate the marketing abilities and promotional capabilities of their distributors and dealers. Most Canadian agents deal with an average of three or four suppliers. Therefore, U.S. firms need to ensure that their dealers will be able to provide adequate product representation and service.

Alternatively, U.S. vendors may choose to have a direct presence in the Canadian market. This can be accomplished by operating a Canadian sales office, or by setting up an affiliated company in Canada. Advantages to the later option include the presence of a highly skilled local security labor force and labor costs that are lower than in the United States.

In the access control industry, as in the whole Canadian security industry, common payment practices are net 30 days. Discounts are normally available if payment is made by the tenth day of the month following shipment. However, open account and extended-term agreements are generally preferred where U.S. suppliers are concerned.

Currently, three national distributors dominate the Canadian access control industry:

- *Burtek Systems Inc*.
  Burtek Systems is a nationwide distributor and importer specializing in commercial sound, alarm, access control and intercom products.
- *Tri-Ed Ltd*.
  Tri-Ed Ltd. is a national distributor with branches all over North America that distributes alarm systems, CCTV devices, and other access control products.
- *ADI*
  ADI is also a national distributor with branches all over North America that distributes burglar and fire alarms, CCTV products, and other access control systems. Production accounts for only 11 percent of its sales.

Major U.S. companies in the market through distributors include Northern Computers, Hirsch and Ingersoll Rand.

It is essential that U.S. companies continue to provide the best technology in their products -- as one industry insider has stated, *"Perhaps, we are finally reaching the era where, in fact, the caliber of the security company will become a much more important consideration than the cost of its services."* In particular, this trend will bode well for more expensive, but best prospect technologies like biometrics in the future.

Market Issues & Obstackes

Canada does not have a comprehensive regulatory scheme for safety and security products. Importers of security alarm products must obtain certification from Underwriter's Laboratories of Canada (ULC), the Canadian Standards Association (CSA), Industry Canada, and/or Factory Mutual Engineers (FM).

However, after eight years of development, Underwriters' Laboratories of Canada (ULC) announced in November 2005 the First Edition of CAN/ULC-S319-05, Electronic Access Control Systems. This standard was approved by the ULC Committee on Security and Burglar Alarm Equipment and Systems, and is dated September 2005. The standard sets new requirements for the construction, performance and operation of access control systems, and provides Canadian security manufacturers, integrators and end users with the parameters and guidelines they need to design, install and implement reliable and sustainable access control systems. ULC S319 sets out a modular approached, based on government and private sector needs, rather than technology that can ensure availability of reliable cost-effective equipment. Although ULC S319 does not include installation standards — which are expected to be published at a later date — it does help security installers and integrators in several ways.

ULC also conducts performance tests and issues approval for newly introduced access control systems. Additionally, like the Canadian Standards Association (CSA), it also tests and certifies a wide range of electrical equipment and appliances, and serves as a source of information for U.S. companies that want to register their products for retail in Canada. CSA electrical certification is mandatory for wired systems or battery-operated equipment that operates on more than 30 volts. CSA also tests access control systems for power hazards, as this is a requirement for all electrical and electronic products, which operate within certain radio frequency bands. U.S. companies should therefore examine closely which testing certification their products need and which testing agency best meets their needs.

To maximize market penetration and comply with Quebec's language laws, instructions, warranties and packaging accompanying access control products sold in Canada should be in both of Canada's official languages, English and French. So if the Quebec rules are followed, companies will meet all the bilingual rules that may be applicable for sales in the other provinces. The Office québécois de la langue française may be contacted for further details on language requirements. Exporters are encouraged to work with a local distributor or major retailer to meet these requirements and ensure proper French-Canadian language usage.

No customs duties or tariffs are levied on qualified U.S.-made access control systems entering Canada. The Canadian Goods and Services tax (GST) of 7 percent on a value-added basis is assessed by Revenue Canada at the time of import, and at each subsequent resale level. Importers are entitled to partially offset their GST payments by collecting and retaining GST payments received from their customers.

Trade Events

Cardware 06
June 13, 2006
Toronto, Ontario

Infosecurity Canada
June 20-21, 2006
Toronto, Ontario

Security Canada Central
October 17-19, 2006

Other North American trade shows and conferences in this sector which attract significant numbers of Canadian visitors are ISC East, to be held October 24-25 in New York City.

Resources & Key Contacts

Canadian Security Association (CANASA) http://www.canasa.org

Advanced Card Technology Canada www.actcda.com

Canadian Advanced Technology Alliance www.cata.ca

SP&T News www.sptnews.ca

Canadian Security Magazine www.canadiansecuritymag.com

For More Information

Connie Irrera, the author of this report at the U.S. Commercial Service in Montreal, Canada, can be contacted via e-mail at: connie.irrera@mail.doc.gov; by phone at 514-398-9695 ext. 2262; by fax at 514-398-0711 or by visiting the website of U.S.C.S. Canada: www.buyusa.gov/canada.

The U.S. Commercial Service — Your Global Business Partner

With its network of offices across the United States and in more than 80 countries, the U.S. Commercial Service of the U.S. Department of Commerce utilizes its global presence and international marketing expertise to help U.S. companies sell their products and services worldwide. Locate the U.S. Commercial Service trade specialist in the U.S. nearest you by visiting http://www.export.gov/.

Disclaimer: The information provided in this report is intended to be of assistance to U.S. exporters. While we make every effort to ensure its accuracy, neither the United States government nor any of its employees make any representation as to the accuracy or completeness of information in this or any other United States government document. Readers are advised to independently verify any information prior to reliance thereon. The information provided in this report does not constitute legal advice.

International copyright, U.S. Department of Commerce, 2006. All rights reserved outside of the United States.